DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

27 March 2003

MEMORANDUM FOR DIRECTOR, NAVY STAFF
DIRECTOR, MARINE CORPS STAFF

Subj: UPDATE OF DON INFORMATION TECHNOLOGY (IT) SYSTEMS REGISTRATION GUIDANCE

Ref: (a) DON CIO memo of 26 Feb 2002
(b) DoD CIO memo of 17 Mar 2003

Encl: (1) Department of the Navy 2003 Information Technology Registration Database Guidance

This memorandum updates reference (a) regarding DON IT Systems Registration, incorporating reference (b) guidance.

The Department currently maintains an Information Technology Registration database to provide an accurate and reliable enterprise-wide inventory. This accuracy is made possible by the diligent efforts of Navy and Marine Corps systems owners maintaining the data regarding their systems. The data in the DON IT Registration database is uploaded to the DoD Registration database quarterly in compliance with various statutory requirements.

Enclosure (1) contains DON IT Systems Registration Guidance, incorporating the recent guidance received from DoD, in reference (b). As a result of the Federal Information Security Management Act (FISMA), DoD and DON IT Registries were expanded last year to include information required for the annual FISMA report to Congress. In addition, new fields have been added this year for which data must be inserted for the FISMA Report.

We note that in many cases, information in the DON IT Registry is incomplete and/or outdated. The following data is especially important to assist all users to meet their responsibilities:

- Up-to-date POC data, including telephone number and e-mail address
- Complete FISMA data, including date of expected certification and accreditation for those systems that have not yet completed the DITSCAP process, as well as all other FISMA fields.

In accordance with the DoD IT Registry Guidance, I am required by 30 April 2003 to certify by letter to the DoD CIO that DON mission critical and mission essential IT systems have been registered in the IT Registry. Therefore, I require written confirmation by 21 April 2003 from the DON Deputy CIO (Navy) and the DON Deputy CIO (Marine Corps) certifying that their respective Mission Critical/Mission Essential IT systems have been registered in the DON IT Registry. I will have the DON IT Registry uploaded to the DoD IT Registry for the next quarterly update with the data as of 30 March 2003.

My point of contact for the DON IT Registry is Ms. Judy McCarthy, 703-602-6845, judy.mccarthy@navy.mil, and for FISMA is Mr. James Collins, 703-602-6202, james.e.collins@navy.mil.

D. M. Wennergren

Copy to:
Immediate Office of the Secretary (AA/USN, ASN(M&RA), ASN(RD&A), ASN(I&E), ASN(FM&C)) only
HQMC DIR C4
CHNAVPERS
COMUSNAVCENT
COMLANTFLT
COMPACFLT
COMUSNAVEUR
COMNAVRESFOR
COMSC
COMNAVMETOCCOM
COMNAVSECGRU
BUMED
COMNAVAIRSYSCOM
COMSPAWARSYSCOM
COMNAVFACENGCOM
COMNAVSUPSYSCOM
COMNAVSEASYSCOM
DIRSSP
ONI
CNET
COMNAVSPECWARCOM
USNA
COMNAVDIST WASHINGTON
FLDSUPPACT
NAVHISTCEN
COMNAVLEGSVCCOM
NAVOBSY
PRESINSURV
OPNAVSUPPACT
COMOPTEVFOR
NAVPGSCOL
COMNAVSAFECEN
NAVSTKAIRWARCEN

Copy to: (continued)
NCTSI
CNR
COMNAVNETSPAOPSCOM
COMNAVSYSMGTACT
DON Deputy CIO (Navy)
DON Deputy CIO (Marine Corps)
DIR NMCI
COMNAVNETWARCOM
OGC
NRL
CNO (N09B, N09BF, N091, N093, N095, N096, N1, N2, N3/N5, N4, N6/N7, N8 only)
NAVCRIMINVSERV
PEO for Air, ASW, Assault and Special Mission Program
PEO for Strike Weapons and Unmanned Aviation
PEO for Space Communications and Sensors Program
PEO for Theater Surface Combatants
PEO for Tactical Aircraft Programs
PEO for Surface Strike
PEO for Mine and Undersea Warfare
PEO for Submarines
PEO for Expeditionary Warfare
PEO for Aircraft Carriers
PEO for Information Technology
DRPM for Strategic Systems Program
DRPM for Advanced Amphibious Assault

Department of the Navy (DON) 2003 Information Technology (IT) Registration Database Guidance

March 2003

Department of the Navy (DON) 2003
Information Technology (IT) Registration Database Guidance

Table of Contents

Department of the Navy (DON)
2003 Information Technology (IT) Registration Database Guidance

Introduction

DoD continues to use the DoD IT Registry as the means to maintain IT system registration, to comply with Congressional requirements and to serve as a technical repository to support CIO assessments. Because this is a continuing Congressional requirement, the DON will continue to use the DON IT Registration Database as the source for collecting the required data and uploading the data to the DoD IT Registry, and for making CIO assessments. This guide is intended to provide Program Managers, system owners, and major claimants with detailed guidance for updating the data in the DON IT Registration Database in preparation for quarterly uploads and annual certification to DoD.

Responsibilities

The DON CIO is responsible for evaluating and ensuring IT and weapon system programs, including National Security Systems (NSS) that contain Mission Critical (MC) or Mission Essential (ME) IT systems comply with the Clinger-Cohen Act, FISMA, IT registration, and other requirements. See Appendix 4 for supporting definitions.

DON Commands are responsible for providing accurate data and updating the DON IT registration database on a quarterly basis by: 30 March, 30 June, 30 September, and 30 December each year. DON commands shall annually certify in writing to their respective DON Deputy CIO, who will in turn certify to DON CIO, that their respective mission critical/mission essential IT systems have been registered in the DON IT Registration Database. DON CIO will upload the data to the DoD IT Registration database quarterly, and annually certify to DoD.

New for 2003

The 2002 DON IT Registration Guidance addressed required system security data pursuant to the Government Information Security Reform Act (GISRA); a new directive from DoD redirects these requirements under auspices of the Federal Information Security Management Act (FISMA). The DON IT Registration database has been recently modified to support additional FISMA requirements.

New FISMA fields added to the database are 'System Life Cycle Costs' and 'Security Controls Tested'. Systems Life Cycle Costs is a YES or NO question and is asking the user to indicate whether their system has the costs of its security controls integrated into the lifecycle cost of the system. The field Security Controls Tested is the date in which the security controls of the systems were last tested. The only other change to FISMA fields is to the value list in the question regarding 'Accreditation Status'. The value 'NA' has been added for those systems that are not applicable. Appendix 3 provides an outline of the DON IT Registry database fields and their definitions.

Federal Information Management Security Act (FISMA)

The E-Government Act of 2002, Title III, contains the Federal Information Security Management Act (FISMA) legislation. FISMA updates the Government Information Security Reform Act (GISRA) legislation that was part of the National Defense Authorization Act for FY 2001, but with minimum changes. FISMA requirements include setting up an information security policy, and conducting monitoring, evaluation, training, and oversight of information security programs in Federal Agencies, as well as an annual report to the Office of Management and Budget (OMB) and Congress.

The IT Registry will be the vehicle for collecting system security status for the annual report. DoD and DON have added new FISMA data fields to the respective IT Registries to incorporate added report requirements. These new fields and their definitions are identified in Appendix 3. Commands are requested to ensure the FISMA fields, including the new set, are updated with accurate and complete information. An added requirement is that if accreditation is not complete and "NONE" is inserted in the Accreditation Status field, the expected date of accreditation be inserted in the Accreditation Date field.

The report to OSD, OMB, and Congress will be taken directly from the DoD IT Registry, updated from the DON IT Registry – hence it is important that data be current and correct.

Statutory Requirements

Section 811 of the Floyd D. Spence National Defense Authorization Act for FY 2001, amended section 2223(a) of title 10, United States Code, to require a consolidated inventory of DoD mission critical and mission essential information systems be maintained; interfaces between these systems and other systems be identified; and contingency plans for responding to a disruption in the operation of any of these systems be developed and maintained. Section 811 also directed the revision of Department of Defense Directive 5000.1, to prohibit the award of any contract for the acquisition of a mission critical or mission essential information technology system until the system is registered with the DoD CIO.

The National Defense Appropriations Act, FY 2000 (Pub L. 106-79), Section 8121(a) provided that after March 31, 2000, none of the funds (including Defense Working Capital Funds) appropriated in the DoD Appropriations Act, FY 2000, may be used for a mission critical (MC) or mission essential (ME) information technology (IT) system (as defined by the Secretary of Defense) that is not registered with the DoD Chief Information Officer

(CIO). Obligation or expenditure of FY 2000 funds for mission critical or mission essential IT systems not registered may result in a potential Antideficency Act violation.

The National Defense Appropriations Act, FY 2001 (Pub L. 106-259), Section 8102(a) continued the requirement to have MC and ME IT systems registered with the DON CIO prior to the use of FY 2001 funds.

The National Defense Appropriations Act, FY 2002 (Pub L. 107-117), Section 8104. (a) requires Financial Management information technology systems to be registered with the DoD Chief Information Officer. None of the funds appropriated in this Act may be used for a MC or ME financial management IT system (including a system funded by the Defense Working Capital Fund) that is not registered with the DON CIO. The section provides that a system shall be considered to be registered by furnishing notice of the system, together with such information concerning the system as the Secretary of Defense may prescribe. A financial management IT system shall be considered a MC or ME IT system as defined by the Under Secretary of Defense (Comptroller). DON commands are requested to continue reporting Financial Management Information Systems in the DON IT Registration Database as was done in the past. When the implementing guidance is received from DoD it will be provided by separate correspondence.

Reporting Requirements

The Secretary of Defense must report to Congress on the status of Section 811(a) implementation. In addition, the DoD will report to OMB on the status of the implementation of the Federal Information Systems Management Act (FISMA).

What must be registered in the DON IT Registration Database

The DON IT Registration Database must contain all MC and ME information technology (IT) systems (including National Security Systems) that are fielded, as well as systems that are being developed and will be fielded in the future. Appendix 3 identifies all data fields that must be entered in the DON IT Registration database.

A financial management IT system shall be considered a mission critical or mission essential IT system, as defined by the Under Secretary of Defense (Comptroller). If the system is determined to be MC or ME it shall be registered in the DON IT Registration database. Until additional guidance is provided by DoD, DON will continue to maintain and keep updated all information on existing financial management IT systems in the DON IT Registry.

System owners/Program Managers (PMs)/Major Claimants are responsible for making mission critical and mission essential information system designations and for reporting these systems (including NSSs) in the DON IT Registration database. The determination for mission essential should be made from the perspective of what is “basic and necessary” for the accomplishment of the overall DON mission.

System owners/PMs/major claimants must validate all system records in the existing DON IT Registration database using the definitions/guidance provided, and updating the system records, as needed. Should any systems be deleted, a listing of such systems with a short rationale for the removal must be attached to your Command certification.

A system must be identified in the DON IT Registration database as a Main System, Active (or new development as appropriate), and IT systems without this information cannot be uploaded to DoD).

"Main" IT systems within the ship or aircraft will be registered as IT systems and should be reported in the DON IT Registration database as Main system, Active (or new development, as appropriate) and IT system.

IT systems integral to missile operation, yet not physically contained within the launched missile, should be registered. Examples of these IT systems include fire control systems and mission planning systems. These systems should be reported as Main System, Active (or new development) as appropriate, and IT system.

All systems that have an OSD Budget Initiative Number (BIN) assigned will be registered, this will include: subsystems, local unique systems, and or networks with an assigned BIN.

Prior to awarding a contract for any acquisition category (ACAT) program for MC or ME IT system, the system must be registered in the DON IT Registration database.

What should NOT be registered in the database

Weapons and platforms (ships or aircraft) ***without*** embedded IT will not be registered in the database. However, MC or ME IT systems on the platform or weapon will be registered.

Missiles are considered to be weapons launched from a platform, but not IT for the purposes of registration of IT systems. Missiles include, but are not limited to Sea Sparrow, HARM, Phoenix, Tomahawk, and Trident. If a missile was previously reported in the DON IT Registration database, the System Type field should appear as "N" (for Non-IT system) to ensure it is not registered as an IT system with DoD.

Subsystems and local unique systems that do not have an OSD BIN assigned will not be registered. Local unique systems are not considered mission critical or mission essential to the overall Combatant Commander or DON mission. As such, they do not need to be registered. Local unique information systems are defined as software applications developed to support local requirements of USN/USMC Bases. Examples of local unique information systems are system features or functionality that were locally added to a centrally managed information system, information systems developed by functional areas of the USN/USMC Base to support their specific mission, and locally developed Internet web pages.

Networks (WANS, MANs, BANs, LANs) that do not have an OSD BIN number assigned will not be registered.

Secret /SCI/Special Access Programs

Systems Classified as Secret shall be registered through the SIPRNET at:
http:// 147.254.40.136.

Special Compartmental Information (SCI) Systems shall be registered separately through:

- USN - Mr. Tim Sydnor (301) 669-2018, tsydnor@nmic.navy.mil.

- USMC - Master Sergeant Richard Corrigan (703) 695-1053, corriganRM@hqmc.usmc.mil.

Special Access Programs (SAP) registration shall be through:
LTCOL Charles Schwarz at the OSD Special Access Program Central Office (SAPCO) at (703) 697-3493, charles.schwarz@osd.mil. (All DON Special Access Programs will follow the guidance issued by the DOD Special Access Program Central Office SAPCO.)

OSD BIN Numbers

IT Systems with OSD BIN numbers must be registered in the DON IT Registration Database. Please contact Mr. Brian Baker-Brent at ASN9FM&C), 703-692-4841, baker.brian@hq.navy.mil if you need assistance on this subject.

Access to the DON IT Registration Database

Our goal is to ensure only authorized personnel with a need to know gain access to the Department of the Navy (DON) information technology (IT) Registration Database. We have established primary points of contact at all Echelon II Navy and Headquarters Marine Corps (HQMC) commands to control who have review/editing privileges.

URL to log on to the DON IT Registration Database:
http://www.don-imit.navy.mil/cca/registration/

Procedures for establishing a user account at the DON IT Registration Database:

1. Applicant will complete the DON IT Registration Database - Account Request Form (Appendix 1).
2. Applicant will submit the completed form to their Echelon II USN/HQMC DON IT Registration Database Primary point of contact (POC) for an approval decision listed in Appendix 2.

3. The Echelon II USN/HQMC DON IT Registration Database POC will review the form for completeness and accuracy, and verify that the applicant has a valid requirement for access. The Echelon II USN/HQMC DON IT Registration Database POC is responsible for maintaining the original file of user access forms. If approval is warranted, the Echelon II USN/HQMC DON IT Registration Database POC will sign the form and forward a signed copy of the form to the DON System Administrator (e-mail or FAX). The DON System Administrator is Mr. Richard Gallagher. Mr. Gallagher may be reached on E-mail Gallagher_Richard@BAH.com, or by office telephone on 703-413-7015, or by FAX on telephone 703-413-7021.
4. The DON System Administrator will process the form and notify the Echelon II USN/HQMC DON IT Registration Database POC and the applicant of the completed action by e-mail within 3 working days.

DON IT Registration Points of Contact

Mr. Mark Mohler
DON Deputy CIO (USN) POC
(703) 601-1200
E-mail: mark.mohler@navy.mil

Ms. Marilyn Stahovic
DON Deputy CIO (USMC) POC
E-mail: stahovicmi@hqmc.usmc.mil

Ms. Judy McCarthy
DON CIO Program Manager (Registration policy)
(703) 602-6845
E-mail: judy.mccarthy@navy.mil

Mr. Richard Gallagher
Technical Database POC (Database, system questions, special reports)
(703) 413-7015
E-mail Gallagher_richard@bah.com

Mr. Jim Collins
DON CIO Information Assurance Team (FISMA policy, data)
(703) 602-6202
E-mail james.e.collins@navy.mil

This guide and additional information regarding this subject also resides on the DON CIO website available at: http://www.don-imit.navy.mil/

Appendix 1 - Account Request Form

DON IT REGISTRATION DATABASE - ACCOUNT REQUEST FORM

ACTION REQUIRED:

□ New User □ Delete User □ Existing User (update user information)

ACCOUNT TYPE:

□ Read/Edit □ Read Only

1. Last Name:____________________ First:________________ MI:____

Command ______________________

Address 1: ____

Address 2: ____

□ Civilian □ Military □ Contractor

2. Commercial Phone: ______________________ DSN Phone: __________________

3. Users E-mail Address ____

4. Requirement for Access: ____

____

____

5. Do you have a Common Access Card? □Yes □No Will you use it to access the system □Yes □No

6. Supervisors Name: ______________________ Supervisors Phone: ________________

7. Authorization (Echelon II Primary DON IT Registration Database POC) □Approve □Disapprove

Echelon II Command: _________________________

Name:____ Phone: _________________

Signature:_____________________________________ Date: _________________

8. Comments: ____

____

INSTRUCTIONS:

1) Applicant will complete the DON IT Registration Database – Account Request Form and obtain their supervisor's signature.

2) Applicant will submit the completed form to their Echelon II DON IT Registration Database point of contact (POC) for an approval decision.

3) The Echelon II DON IT Registration Database POC will review the form for completeness and accuracy, and verify that the applicant has a valid requirement for access. The Echelon II DON IT Registration Database POC is responsible for maintaining the original file of user access forms. If approval is warranted, the Echelon II DON IT Registration Database POC will sign the form and forward a signed copy of the form to the DON System Administrator (e-mail or FAX). The DON System Administrator is Mr. Richard Gallagher. He may be reached on E-mail Gallagher_Richard@BAH.com, office telephone is 703-413-7015, FAX telephone is 703-413-7021.

4) The DON System Administrator will process the form (establish account access)and notify the Echelon II DON IT Registration Database POC and the applicant of the completed action by e-mail within 3 working days.

Common Access Card (Optional): The DON IT Registration Database system has been designed and developed to support the 'new' Common Access Card (CAC). DON encourages users to use their CAC to access the database. Your user name and password will still be required, but only to initiate your first log on. After initial logon, only your CAC and PIN code will be needed to log on to the database. Users who do not have a CAC card can still access the database with a user id and a password. Please contact the System Administrator if you need assistance.

For assistance contact Mr. Richard Gallagher on gallagher_richard@bah.com or telephone 703-413-7105.

As of: 1-31-2002

Appendix 2 - Primary Command Points of Contact

IT REG CLAIMANT	IT REG POC	POC ROLE	PHONE	IT REG EMAIL
AAUSN	Mr. Edward Peretich	User	(202) 433-0733	peretich.edward@hq.navy.mil
AAUSN	Mr. Gary Wyckoff	Primary PM	(703) 695-6191	wyckoff.gary@hq.navy.mil
BUMED	LCDR Lynda Race	Primary PM	(301) 319-1099	lmrace@us.med.navy.mil
BUMED	Ms. Sue Elberson	User	(301) 319-1138	slelbertson@US.MED.NAVY.MIL
BUPERS	Ms. Melody Potter	Primary PM	(901) 874-3513	melody.potter@navy.mil
COMLANTFLT	Ms. Frances Stefonich	Primary PM	(757) 836-6932	FRANCES.STEFONICH@NAVY.MIL
COMPACFLT	Mr. Marty Smith	Primary PM	(808) 474-1269	smithwm@cpf.navy.mil
COMUSNAVEUR	Capt. Don Kerrigan	Primary PM	(011)44207 514-4836	cnen6@naveur.navy.mil
CNET	Ottendorfer, EW	User	(850) 452-4044	william-O.ottendorfer@cnet.navy.mil
CNET	Mr. Curt Jones	Primary PM	(850) 452-4098	curt-l.jones@cnet.navy.mil
CNMOC	Mr. Sandra Davis	User	(228) 688-4470	davisS@cnmoc.navy.mil
CNMOC	Mr. Robert Starek	User	(228) 688-5993	starekr@cnmoc.navy.mil
CNMOC	Ms. B.J. Dauro	Primary PM	(228) 688-4518	daurob@cnmoc.navy.mil
CNMOC	Mr. Thomas Nabors	User	(228) 688-5248	naborst@cnmoc.navy.mil
CNO (09BF)	Mr Craig Williams	Primary PM	(202) 685-1507	craig.a.williams@navy.mil
CNR	Dr. John McLean	Primary PM	(202) 767-29(	mclean@itd.nrl.navy.mil
COMNAVRESFOR	Mr. Neil Clement	Primary PM	(504) 678-6102	clement@cnrf.navy.mil
COMSC	Mr. Ed Meade	Primary PM	(202) 685-5600	ed.meade@msc.navy.mil
DIRSSP	Mr. Bill Hyre	Primary PM	(202) 764-1432	sp164@ssp.navy.mil
HQMC	Ms. Patricia Wallace	Primary PM	(703) 614-9792	wallacepl@msc.navy.mil
HQMC	Ms. Marilyn Stahovic	Primary PM	(703) 614-9792	stahovicmj@hqmc.usmc.mil
MSC	Mr. James Dykes	User	(202) 685-5327	jim.dykes@msc.navy.mil

IT REG CLAIMANT	IT REG POC	POC ROLE	PHONE	IT REG EMAIL
MSC	Mr. Ralph Marks	Primary PM	(202) 685-5339	ralph.marks@msc.navy.mil
NAVAIR	Ms. Sharon Gensib	User	(301) 757-6444	Sharon.Gensib@Navy.mil
NAVAIR	Ms. Kathy Steele	Primary PM	(301) 342-4799	Kathy.steele@navy.mil
NAVAIR	Ms. Liz Medved	User	(301) 342-7412	medvedem@navair.navy.mil
NAVAIR	Mr. Richard Ferguson	User	(301) 757-8781	fergusonrb@navair.navy.mil
NAVFAC	Ms. Margot Lynn	Primary PM	(202) 685-9031	lynnm@navfac.navy.mil
NAVFAC	Mr. Jim Carberry	User	(202) 685-9037	carberryjj@navfac.navy.mil
NAVFAC	Mr. Mary Jean Snead	Primary PM	(202) 685-9039	sneadm@navfac.navy.mil
NAVSEA	Ms. Mary Pearson	Primary PM	(202) 781-0977	pearsonmw@navsea.navy.mil
NAVSECGRU	Mr. Dave Bodin	Primary PM	(240) 373-3239	dbodin@hq.cnsg.navy.mil
NAVSUP	Mr. Mark Porterfield	Primary PM	(717) 605-6971	mark.r.porterfield@navy.mil
NAVSUP	Ms. Pamela Wenner	User	(717) 605-7535	pamela.d.wenner@navy.mil
NCIS	Mr. William VonStorch	Primary PM	(202) 433-5482	bvonstor@ncis.navy.mil
NNSOC	Ms. Michelle Tolson	User	(805) 989-7807	tolsonm@satops.mugu.navy.mil
NNSOC	Ms. Nancy Mullen	User	(540) 653-5537	unmullen@nsc.navy.mil
NNSOC	Ms. Diane Jacobs	Primary PM	(540) 653-5548	jacobs@nsc.navy.mil
NNSOC	Mr. Richard Roussin	User	(202) 764-0916	richard.roussin@navy.mil
ONI	Mr. Robert Oldach	Primary PM	(301) 669-5227	roldach@nmic.navy.mil
ONR	Mr. Timothy Warren	Primary PM	(703) 696-2771	warrent@onr.navy.mil
PEO (IT)	Ms. Mary Lawson-Hines	Primary PM	(703) 602-3120	Mary.Hines1@navy.mil
SPAWAR	Mr. Scott Saunders	User	(858) 537-0573	scott.saunders@navy.mil
SPAWAR	Ms. Sarah Lamades	Primary PM	(619) 524-7008	sarah.lamades@navy.mil
USNO	LCDR Scott Diaz	Primary PM	(202) 762-1537	diaz.scott@usno.navy.mil

Appendix 3- DON CIO IT Registration Data Fields

* New or modified FISMA fields

DONCIO FIELD NAME	FIELD SIZE	VALUES	FIELD DESCRIPTION
APPLIC ID	20	Auto	The distinct System Identification Number or Code used on the Component's database for this MC/ME IT system.
MISSION CRITICAL	2	Value List	The mission criticality of this IT system. Acceptable values are MC or ME or OT (Other)
ACRONYM	30	Text	A shortened or commonly used name or abbreviation (upper case) for this MC/ME IT System.
SYSTEM NAME	100	Text	The full descriptive name for this MC/ME IT system (upper case).
SYSTEM DESCRIPTION	255	Text	A free form text description of the system, its function, and uses.
ACQUISITION CATEGORY	3	Value List	The acquisition category for this program.
FUNCTIONAL AREA	50	Value List	Relates to the functions under which this particular MC/ME IT system is reported.
SECONDARY FUNCTIONAL AREA	50	Value List	For use if this MC/ME IT system has a secondary function.
TERTIARY FUNCTIONAL AREA	50	Value List	For use if this MC/ME IT system has a tertiary function.
PM NAME	50	Text	First and Last name of Program Manager (PM) or POC for this MC/ME IT System
PM TITLE	10	Value List	Rank, Grade, and Title of PM or POC or Systems Manager.
MAJOR COMMAND	50	Text	Organization of PM or POC or Systems Manager.
PM COMMERCIAL PHONE	18	Text	Commercial phone number of PM or POC or Systems Manager.
PM DSN PHONE	18	Text	Defense Switched Network phone number of PM or POC or Systems Manager.
PM EMAIL	100	Text	Email address of PM or POC or Systems Manager.
BIN	6	Text	Insert the Budget Initiative Number if it exists, from the Information Technology Management Application (ITMA) Database.
INTERFACES IDENTIFIED	3	Yes, No, NA	Indicates if the system interfaces between this MC/ME IT system and other systems have all been identified. Acceptable values are **Yes, No, or NA.**
MAIN SYSTEM	11	Value List	Only "MAIN" type systems will be reported to DOD. Exceptions: see BIN, below
SYSTEM TYPE	34	Value List	Only "IT System, Weapon System (Which includes IT), and Platform (Which includes IT)" will be reported to DOD. Exceptions: see BIN, below
CONTINGENCY PLAN IN PLACE	3	Yes, No, NA	Indicates if a contingency plan is in place to account for disruptions in the operations of this system. Acceptable values are **Yes, No, or NA.**
CCA CONFIRMATION or CERTIFICATION DATE	8	DATE	On what date was the CCA Confirmation or Certification Complete?
MILESTONE REVIEW DATE	8	DATE	What is the date of the next Milestone Review? This field is applicable if system is an ACAT 1, 1A, 3, or 4 category system.
CONTRACT AWARD DATE	8	DATE	What is the date of the next contract award? This field is applicable if system is an ACAT 1, 1A, 3, or 4 category system.
* ACCREDITATION STATUS	10	Value List	Has your system undergone a certification and accreditation process and if so, what is its current status?
ACCREDITATION DATE	8	Date	Accreditation Date:

DONCIO FIELD NAME	FIELD SIZE	VALUES	FIELD DESCRIPTION
ACCREDITATION VEHICLE	10	Value List	What C&A process was used to grant the current C&A?
FORMAL DOCUMENTATION	3	Yes, No	If your system has a C&A, do you have formal documentation that indicates the specifics of the C&A process?
SYSTEM SECURITY AUTHORIZATION AGREEMENT (SSAA) STATUS	4	Value List	What phase is the SSAA associated with your system in? The phases of the SSAA are based on DITSCAP definitions.
DAA NAME	50	Text	Designated Approving Authority (DAA)
DAA TITLE	100	Text	What is the contact information for the DAA that granted your system's latest C&A status?
DAA_ORG	50	Text	Organization of PM or POC or Systems Manager.
DAA PHONE	18	Text	DAA Commercial phone number.
DAA EMAIL	100	Text	DAA Email address.
CONTINGENCY PLAN / CONTINUITY OF OPERATIONS (COOP)	8	Date	When was the last time that your system's contingency plan or COOP was exercised?
ACCESS CONTROLS	3	Yes, No	Does your system have measures in place that control access and prevent the circumvention of the security software and application controls?
ADMINISTRATIVE CONTROLS	3	Yes, No	Does your system have measures in place that ensure the proper administration of your system to include identification of users, groups, and their privileges as well as the capability to produce system activity audit logs?
SECURITY INCIDENT RESPONSE (CSIRT)	3	Yes, No	Does your system have controls in place to recognize, report, monitor and efficiently handle incidents, and is there capability to share this information with appropriate organizations?
VIRUS PROTECTION	3	Yes, No	Does your system have virus protection and data integrity controls that protect data from accidental or malicious alteration or destruction and that protect your system from infection from malicious computer viruses?
HARDWARE / SOFTWARE MAINTENANCE PLAN	3	Yes, No	Does your system have controls that are used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes?
RISK MANAGEMENT PLAN	3	Yes, No	Does your system have a risk management plan that identifies the risks and vulnerabilities to the system, recognizes the sensitivity of the data and lays out a plan to mitigate those risks and vulnerabilities?
* SYSTEM SECURITY PLAN	3	Yes, No	Does your system has a system security plan that provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements? Does the plan delineate responsibilities and expected behavior of all individuals who access the system?
SYSTEM LIFE CYCLE PLAN	3	Yes, No	Does your system have a life cycle plan that discusses at minimum the basic life cycle phases?
*** SYSTEM LIFE CYCLE COSTS**	3	Yes, No	Indicate whether your system has the costs of its security controls intergraded into the lifecycle cost of the system. YES NO
*** SECURITY CONTROLS TESTED**	8	Date	Indicate the last date in which the security controls were tested.
RECORD TYPE	64	Value List	Indicate the classification for record in the Registry (e.g. System, Application, Network, or Acquisition Program)
LIFE CYCLE	64	Value List	Indicate the system life cycle phase for this record entity.

Appendix 4 – Key Definitions

Information System. An 'information system' is defined in Section 3502, Title 44, US Code (8): the term 'information system' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

Information Technology. The accepted DoD definition of 'Information Technology (IT)' contained within Section 5002(3), Title 40 U.S. Code 1401 (also known as the Clinger-Cohen Act of 1996): (3) (A) The term 'information technology' means "any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency."

> (B) The term 'information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services) and related services. The term "IT" also includes National Security Systems (NSSs).

National Security System. A "national security system" is defined in Section 5142; Title 40 U.S. Code 1401 and means "any telecommunications or information system operated by the United States Government, the function, operation, or use of which--

1. involves intelligence activities;
2. involves crypto logic activities related to national security;
3. involves command and control of military forces;
4. involves equipment that is an integral part of a weapon or weapons system; or
5. subject to subsection (b), is critical to the direct fulfillment of military or intelligence missions (this does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications))."

Major Automated Information System (MAIS). An AIS that is designated by ASD (C3I) as a MAIS, or estimated to require program costs in any single year in excess of $32 million in fiscal year (FY) 2000 constant dollars, total program costs in excess of $126 million in FY 2000 constant dollars, or total life cycle costs in excess of $378 million in FY 2000 constant dollars. For the purposes of determining whether an AIS is a MAIS, the following shall be aggregated and considered a single AIS:

1. The separate AISs that constitute a multi-element program.
2. The separate AISs that make up an evolutionary or incrementally developed program.
3. The separate AISs that make up a multi-DoD Component AIS program.

Mission Critical System. A "mission critical information system" is a system that meets the definition of "information system" and "national security system" in the Clinger-Cohen Act, the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Note: A component head, a CINC, or their designee should make the designation of "mission critical") A "mission critical information technology system" has the same meaning as a "mission critical information system."

SECNAV memo of 16 Mar 2001 authorized DON System Owners, Program Managers, and major claimants to make mission critical or mission essential information system designations.

Mission Essential Information System. A system that meets the definition of "information system" in the Clinger-Cohen Act, that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Note: A component head, a CINC, or their designee should make the designation of "mission essential"). A "mission essential information technology system" has the same meaning as a "mission essential information system."

SECNAV memo of 16 Mar 2001 authorized DON System Owners, Program Managers, and major claimants to make mission critical or mission essential information system designations.

Weapon System. An item or set of items that can be used directly by warfighters to carry out combat support missions to include tactical communication systems.